Advisory Alert

Alert Number: AAA20240911 **Date:** September 11, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Improper Authentication Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Citrix	**High**	Privilege Escalation Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Fortiguard	**High**, Medium	Multiple Vulnerabilities
Intel	**High**, Medium	Multiple Vulnerabilities
Lenovo	**High**, Medium	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-32840, CVE-2024-32842, CVE-2024-32843, CVE-2024-32845, CVE-2024-32846, CVE-2024-32848, CVE-2024-34779, CVE-2024-34783, CVE-2024-34785, CVE-2024-29847)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation could lead to unauthorized access to the EPM core server. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager - 2024 Ivanti Endpoint Manager - 2022 SU5 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Improper Authentication Vulnerability (CVE-2024-41730)
Description	SAP has issued security updates addressing Improper Authentication Vulnerability that exist in in their products. **CVE-2024-41730 -** In SAP BusinessObjects Business Intelligence Platform, if Single Signed On is enabled on Enterprise authentication, an unauthorized user can get a logon token using a REST endpoint. The attacker can fully compromise the system resulting in High impact on confidentiality, integrity and availability. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP BusinessObjects Business Intelligence Platform, Versions - ENTERPRISE 430, 440
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2024.html

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-43469, CVE-2024-38119, CVE-2024-38259, CVE-2024-38258, CVE-2024-38246, CVE-2024-38243, CVE-2024-38237, CVE-2024-38235, CVE-2024-38217, CVE-2024-38014, CVE-2024-37341, CVE-2024-38254, CVE-2024-38249, CVE-2024-38240, CVE-2024-37980, CVE-2024-38194, CVE-2024-43495, CVE-2024-43491, CVE-2024-43487, CVE-2024-30073, CVE-2024-43479, CVE-2024-43476, CVE-2024-43475, CVE-2024-43470, CVE-2024-43466, CVE-2024-43461, CVE-2024-43458, CVE-2024-43457, CVE-2024-43455, CVE-2024-43454, CVE-2024-38045, CVE-2024-21416, CVE-2024-38263, CVE-2024-38260, CVE-2024-38257, CVE-2024-38248, CVE-2024-38247, CVE-2024-38245, CVE-2024-38244, CVE-2024-38239, CVE-2024-38238, CVE-2024-38234, CVE-2024-38233, CVE-2024-38232, CVE-2024-38231, CVE-2024-38228, CVE-2024-38227, CVE-2024-38226, CVE-2024-38225, CVE-2024-38046, CVE-2024-37965, CVE-2024-43465, CVE-2024-43492, CVE-2024-43482, CVE-2024-43474, CVE-2024-43467, CVE-2024-43464, CVE-2024-43463, CVE-2024-38256, CVE-2024-38253, CVE-2024-38252, CVE-2024-38250, CVE-2024-38242, CVE-2024-38241, CVE-2024-38236, CVE-2024-38230, CVE-2024-38188, CVE-2024-38220, CVE-2024-38216, CVE-2024-38018, CVE-2024-26191, CVE-2024-26186, CVE-2024-37342, CVE-2024-37337, CVE-2024-37339, CVE-2024-37340, CVE-2024-37335, CVE-2024-37966, CVE-2024-37338)
Description	Microsoft has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Remote Code Execution, Web Security Feature Bypass, Information Disclosure. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Azure CycleCloud 8.4.2 Azure CycleCloud 8.4.1 Azure CycleCloud 8.4.0 Azure CycleCloud 8.3.0 Azure CycleCloud 8.2.1 Azure CycleCloud 8.2.2 Azure CycleCloud 8.1.1 Windows 11 Version 24H2 for ARM64-based Systems Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2012 R2 (Server Core installation) Windows 10 Version 22H2 for x64-based Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Microsoft SQL Server 2019 for x64-based Systems (CU 28) Microsoft SQL Server 2022 for x64-based Systems (CU 14) Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems	Microsoft SQL Server 2022 for x64-based Systems (GDR) Microsoft SQL Server 2017 for x64-based Systems (CU 31) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Microsoft SQL Server 2019 for x64-based Systems (GDR) Microsoft SQL Server 2017 for x64-based Systems (GDR) Azure Web Apps Windows 10 for 32-bit Systems Windows 10 Version 21H2 for 32-bit Systems Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows 11 Version 24H2 for x64-based Systems Power Automate for Desktop Microsoft Dynamics 365 (on-premises) version 9.1 Azure Network Watcher VM Extension for Windows Azure CycleCloud 8.6.3 Azure CycleCloud 8.6.2 Azure CycleCloud 8.6.1 Azure CycleCloud 8.5.0 Azure CycleCloud 8.1.0 Azure CycleCloud 8.0.2 Azure CycleCloud 8.0.1 Azure CycleCloud 8.6.0 Azure CycleCloud 8.0.0 Azure CycleCloud 8.2.0 Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Microsoft Publisher 2016 (64-bit edition) Microsoft Publisher 2016 (32-bit edition) Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions Microsoft Dynamics 365 Business Central 2023 Release Wave 2 Microsoft Dynamics 365 Business Central 2024 Release Wave 1 Microsoft Dynamics 365 Business Central 2023 Release Wave 1 Microsoft Excel 2016 (64-bit edition) Microsoft Excel 2016 (32-bit edition) Microsoft Office LTSC for Mac 2021 Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Office Online Server Microsoft AutoUpdate for Mac Outlook for iOS Microsoft Visio 2016 (64-bit edition) Microsoft Visio 2016 (32-bit edition) Microsoft Office for Universal Microsoft Office for Android Azure Stack Hub
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Sep

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerabilities (CVE-2024-7889, CVE-2024-7890)
Description	Citrix has released security updates addressing Privilege Escalation vulnerabilities that exist in their products. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix Workspace app for Windows versions Prior to 2405 Citrix Workspace app for Windows versions Prior to 2402 LTSR CU1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/s/article/CTX691485-citrix-workspace-app-for-windows-security-bulletin-cve20247889-and-cve20247890?language=en_US

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Information Disclosure, Denial of service, Improper access control, Execute unauthorized code or commands. Suse advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5, 15.6 Public Cloud Module 15-SP5, 15-SP6 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 12 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243189-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243190-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243194-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243195-1

Affected Product	**Fortiguard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35282, CVE-2024-31490, CVE-2024-21753, CVE-2024-4863, CVE-2024-33508, CVE-2023-44254, CVE-2022-45856, CVE-2024-31489, CVE-2024-36511)
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Information Disclosure, Denial of service, Improper access control, Execute unauthorized code or commands. Fortiguard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-139 • https://www.fortiguard.com/psirt/FG-IR-24-051 • https://www.fortiguard.com/psirt/FG-IR-23-362 • https://www.fortiguard.com/psirt/FG-IR-24-048 • https://www.fortiguard.com/psirt/FG-IR-24-123 • https://www.fortiguard.com/psirt/FG-IR-23-204 • https://www.fortiguard.com/psirt/FG-IR-22-230 • https://www.fortiguard.com/psirt/FG-IR-22-282 • https://www.fortiguard.com/psirt/FG-IR-22-256

Affected Product	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41833, CVE-2024-28170, CVE-2024-21871, CVE-2024-36261, CVE-2023-25546, CVE-2024-34545, CVE-2024-21829, CVE-2024-21781, CVE-2024-36247, CVE-2024-23984, CVE-2024-33848, CVE-2023-43626, CVE-2024-32666, CVE-2023-23904, CVE-2023-22351, CVE-2023-43753, CVE-2024-32940, CVE-2024-34543, CVE-2024-23599, CVE-2023-42772, CVE-2024-24968, CVE-2024-34153)
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Escalation of Privilege, Denial of Service, Information Disclosure. Intel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00926.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01071.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01097.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01103.html

Affected Product	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33164, CVE-2023-22351, CVE-2023-23904, CVE-2023-25546, CVE-2023-41833, CVE-2023-42772, CVE-2023-43626, CVE-2023-43753, CVE-2024-20021, CVE-2024-21781, CVE-2024-21829, CVE-2024-21871, CVE-2024-21993, CVE-2024-23599, CVE-2024-23984, CVE-2024-24968, CVE-2024-3100, CVE-2024-33016, CVE-2024-33051, CVE-2024-45101, CVE-2024-45102, CVE-2024-45103, CVE-2024-45104, CVE-2024-45105, CVE-2024-4550, CVE-2024-7756, CVE-2024-8059, CVE-2024-8278, CVE-2024-8279, CVE-2024-8280, CVE-2024-8281)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Arbitrary Code Execution, Denial of Service, Escalation of Privilege, Information Disclosure. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.lenovo.com/us/en/product_security/LEN-172051 • https://support.lenovo.com/us/en/product_security/LEN-167313 • https://support.lenovo.com/us/en/product_security/LEN-167072 • https://support.lenovo.com/us/en/product_security/LEN-165524 • https://support.lenovo.com/us/en/product_security/LEN-165230 • https://support.lenovo.com/us/en/product_security/LEN-154748

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37397, CVE-2024-8191, CVE-2024-8320, CVE-2024-8321, CVE-2024-8322, CVE-2024-8441, CVE-2024-8190, CVE-2024-8012, CVE-2024-44105, CVE-2024-44104, CVE-2024-44107, CVE-2024-44103, CVE-2024-44106)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Privilege Escalation, leak API secrets. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager - 2024 Ivanti Endpoint Manager - 2022 SU5 and earlier Ivanti IWC - 10.18.0.0 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Workspace-Control-IWC?language=en_US

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2013-3587, CVE-2022-0778, CVE-2023-0215, CVE-2023-0286, CVE-2024-33003, CVE-2024-41728, CVE-2024-41729, CVE-2024-42371, CVE-2024-42378, CVE-2024-42380, CVE-2024-44112, CVE-2024-44113, CVE-2024-44114, CVE-2024-44115, CVE-2024-44116, CVE-2024-44117, CVE-2024-44120, CVE-2024-44121, CVE-2024-45279, CVE-2024-45280, CVE-2024-45281, CVE-2024-45283, CVE-2024-45284, CVE-2024-45285, CVE-2024-45286)
Description	SAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Cross-Site Scripting, Arbitrary Code Execution. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Student Life Cycle Management (SLcM), Versions – 617, 618, 800, 802, 803, 804, 805, 806, 807, 808 • SAP S/4HANA eProcurement, Versions - SAP_APPL 606, SAP_APPL 617, SAP_APPL 618, S4CORE 102, S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108 • SAP S/4 HANA, Version – 900 • SAP Replication Server, Versions - 16.0.3, 16.0.4 • SAP Production and Revenue Accounting (Tobin interface), Versions - S4CEXT 106, S4CEXT 107, S4CEXT 108, IS-PRA 605, IS-PRA 606, IS-PRA 616, IS-PRA 617, IS-PRA 618, IS-PRA 800, IS-PRA 801, IS-PRA 802, IS-PRA 803, IS-PRA 804, IS-PRA 805 • SAP NetWeaver BW (BEx Analyzer), Versions - DW4CORE 200, DW4CORE 300, DW4CORE 400, SAP_BW 700, SAP_BW 701, SAP_BW 702, SAP_BW 731, SAP_BW 740, SAP_BW 750, SAP_BW 751, SAP_BW 752, SAP_BW 753, SAP_BW 754, SAP_BW 755, SAP_BW 756, SAP_BW 757, SAP_BW 758 • SAP NetWeaver AS Java (Logon Application), Version - 7.50 • SAP NetWeaver AS for Java (Destination Service), Versions - 7.50 • SAP NetWeaver Application Server for ABAP and ABAP Platform, Version – 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 912 • SAP NetWeaver Application Server for ABAP (CRM Blueprint Application Builder Panel), Versions – 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, 75I • SAP for Oil & Gas, Versions – 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807, 807 • SAP Commerce Cloud, Versions - HY_COM 1808, 1811, 1905, 2005, 2105, 2011, 2205, COM_CLOUD 2211 • SAP Commerce Cloud, Version - COM_CLOUD 2211 • SAP BusinessObjects Business Intelligence Platform, Version – 430 • SAP Business Warehouse (BEx Analyzer), Versions - DW4CORE 200, DW4CORE 300, DW4CORE 400, SAP_BW 700, SAP_BW 701, SAP_BW 702, SAP_BW 731, SAP_BW 740, SAP_BW 750, SAP_BW 751, SAP_BW 752, SAP_BW 753, SAP_BW 754, SAP_BW 755, SAP_BW 756, SAP_BW 757, SAP_BW 758 • SAP NetWeaver Enterprise Portal, Version - 7.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2024.html

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.